DOI: https://doi.org/10.15688/jvolsu2.2024.3.10

UDC 81’33
LBC 81.1

Submitted: 09.02.2024
Accepted: 09.04.2024

NEW USES FOR LINGUISTIC STEGANOGRAPHY

Andrey V. Dzhunkovskiy

Moscow State Linguistic University, Moscow, Russia

Abstract. The development of modern linguistic steganography and steganalysis technologies creates new opportunities for use cases to be discovered. Our previous research points to high viability of methods such as trigger-container implementation for the traditional goal of covert information relay. While the findings were significant, it appears that linguistic steganography may have additional applications unrelated to this traditional use case. We aim to analyze how these technologies may be beneficially used in VR-environments, digital governance and for recreational purposes and how these advancements give rise to new speech practices. By investigating the broader implications of linguistic steganography, we hope to uncover innovative ways in which this technology can be harnessed to improve information security, facilitate immersive experiences, and contribute to the development of more sophisticated language-based communication strategies. Using linguistic steganography in VR can improve user experience, ensure sensitive information relay, create new game scenarios. In digital governance these technologies can be used to protect data, ensure secure communications and develop new methods of content analysis. In entertainment, linguistic steganography can be a useful tool for creating riddles, ciphers, and alternative modes of communication in games and other entertainment products. All this gives a new impetus to the development of language practices and prospects for further research in this area.

Key words: steganography, VR, trigger-containers, digital governance, applied linguistics.

Citation. Dzhunkovskiy A.V. New Uses for Linguistic Steganography. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 2. Yazykoznanie* [Science Journal of Volgograd State University. Linguistics], 2024, vol. 23, no. 3, pp. 124-133. DOI: https://doi.org/10.15688/jvolsu2.2024.3.10

УДК 81’33
ББК 81.1

Дата поступления статьи: 09.02.2024
Дата принятия статьи: 09.04.2024

НОВЫЕ СФЕРЫ ПРИМЕНЕНИЯ МЕТОДОВ ЛИНГВИСТИЧЕСКОЙ СТЕГАНОГРАФИИ

Андрей Владимирович Джунковский

Московский государственный лингвистический университет, г. Москва, Россия

Аннотация. Развитие современных технологий лингвистической стеганографии (скрытой передачи информации) и стегоанализа (обнаружения фактов передачи скрытой информации) позволяет выявить для них новые сферы применения. В статье рассматриваются вопросы о том, как стеганографические технологии могут быть использованы в виртуальной реальности, сфере цифрового управления, развлекательной индустрии и как эти технологии порождают новые речевые практики. Показано, что добавление лингвистической стеганографии в виртуальные среды может улучшить взаимодействие пользователей, обеспечить безопасность передачи конфиденциальной информации и создать новые сценарии для игр. В цифровом управлении возможно применение технологий скрытой передачи информации для защиты данных, обеспечения безопасности коммуникаций и развития новых методов анализа контента. Установлено, что в области развлечений лингвистическая стеганография может стать эффективным инструментом для создания нетривиальных загадок, шифров и альтернативных способов общения в играх и других развлекательных продуктах. Охарактеризованы новые языковые практики, такие как использование стеганографически сокрытой информации во время общения в VR-среде, импульсом развития которых послужили технологии стеганографии. Намечены перспективы для дальнейших исследований в данной области.

Ключевые слова: стеганография, виртуальная реальность, триггер-контейнеры, цифровое управление, прикладная лингвистика.

Цитирование. Джунковский А. В. Новые сферы применения методов лингвистической стеганографии // Вестник Волгоградского государственного университета. Серия 2, Языкознание. – 2024. – Т. 23, № 3. – С. 124–133. – (На англ. яз.). – DOI: https://doi.org/10.15688/jvolsu2.2024.3.10

Introduction

One of the issues that the field of applied linguistics continuously aims to solve is that of concealing information. This is often addressed through various linguistic techniques and strategies. One common method involves employing euphemisms, which are more pleasant or neutral expressions used in place of potentially sensitive or offensive terms. By substituting harsh or direct language with euphemistic alternatives, individuals can communicate sensitive information with more tact and diplomacy. Another approach is through code-switching, where speakers alternate between different languages or dialects to conceal information from those who do not understand a particular code. This practice is frequently observed in multilingual communities or situations where covert communication is necessary. Additionally, the use of jargon or specialized terminology within specific professions or subcultures can serve as a form of concealing information from outsiders who are not privy to the specialized language codes. These linguistic tools and strategies play a crucial role in facilitating effective communication while ensuring the sensitive information remains hidden or subtly conveyed.

One step further from that in terms of complexity are linguistic cryptography and steganography. Linguistic cryptography is, in essence, a highly advanced way of code-switching in order to conceal information from those without special access. This is achieved through converting plain text with a cypher that makes it unreadable to the naked eye. This is often sufficient for sender and receiver of the message, however, to an expert, and even to many talented amateurs, the fact that a cypher has been used is evident. This bring us to a dilemma: a cypher is an affront to human curiosity, so even if no one wished to gain access to the message hidden within in the first place, its coming to light creates a desire for 3rd parties to crack the encoding and gain access.

Steganography is the art, craft and science of covertly relaying confidential information without using cyphers. The aim is to hide the very fact that a confidential message is being relayed. Steganalysis deals with trying to uncover or destroy these confidential messages for the purposes of either gaining unauthorized access to confidential information or disrupting the act of communication between the sender and the recipient [Wayner, 2009, pp. 27-30].

It would be optimal for us to elucidate the commonly used terminology in the field before proceeding. “Stego” means the secret message. A “Container” is the overt message or part of the message that contains the secret message. An attempt to gain unauthorized access to destroy stego is called an “Attack”. “Steganology” is the complex approach that encompasses steganography, steganalysis and their underlying theoretical frameworks, as well as various meta-approaches necessary to improve upon existing methods. Linguistic steganography can be used in written texts [Potapova, 2002] or speech [Potapova, 2010].

It should be emphasized that the very nature of steganography leaves its mark on the principles of steganalysis. While using cryptotechnologies the fact of hiding information is explicit and the analyst can a priori attempt to decode the message [Alferov, Zubov, Kuzmin, 2012], in the case of stego use the algorithm is different. Due to the fact that the steganalyst constantly works in conditions of uncertainty about what text may contain stego and whether it in fact contains it, when signs of stego are detected, the most common attack method is to distort the container or destroy the entire message.

While steganography itself is not a new invention and has been widely used throughout history, it is only recently that researchers started investigations into optimizing existing methods and creating new ones based on experimental data. This coincides with rapid development of certain technologies that might benefit from applying these steganography methods. We will provide

an overview of existing and potential use cases for these methods in virtual reality, digital governance and recreation. While none of these three fields are new or groundbreaking, it appears that they are successfully withstanding the test of time and becoming more commonplace around the world, which makes investigating their interaction with steganography worthwhile.

Material and methods

We have done some prior research in the field of linguistic steganography and steganalysis. When we set out to conduct it, it was quickly discovered that linguistic steganology lacked the necessary terminology, framework and methods to apply empirical analysis and describe the results in a way that would be beneficial for praxis. This is not to say that steganography did not achieve its intended goals, but rather that the approach was less scientific and more craft-like [Van Tilborg (ed.), 2014]. The veracity of this statement applies fully to Russian but may also be applicable to linguistic steganography using other languages. We are fairly confident that some of the framework we created in the course of our research is transferable to steganography using other languages.

We have previously introduced a three-stage steganalysis methodology for Russian written texts that may hypothetically be used for other languages [Dzhunkovskiy, 2018], a classification of container localizations, created the term "trigger-container", described the framework for using experimental methods to create a prognosis of how efficient different container localizations may be for the purposes of steganography, tested the aforementioned method [Potapova, Dzhunkovskiy, 2020], and created an algorithm based on this data for the purposes of text watermarking inspired by the work of some of our fellow researchers [Kamaruddin et al., 2018].

Having conducted this research, we began to suspect that it may have additional uses in the modern post-pandemic world. We decided to look into VR, digital governance and recreation. All of these fields are heavily digitized, remote and seem to be stable trends which piqued our interest.

As was mentioned prior, none of these fields are new, but they are, at the same time, innovative, which adds to the possibilities of finding uses for steganography in them.

VR as we understand it nowadays was created in the 1950s, and while it was successfully used for the purposes of training and simulation, consumer-grade VR sets only became viable around 2010 with the release of the Oculus Rift prototype. It is rapidly growing to this day (History...).

Digital governance is another global trend that existed for some time, but has been bolstered by the pandemic. It became evident that digitalization of services (including the services a government provides) goes beyond creating convenience, and can also create an important contingency for scenarios where physical interactions are undesirable, suboptimal or simply dangerous.

Lastly, we elected to analyze how steganography is and may be used for the purposes of recreation. The video game industry has been rapidly growing and its revenue currently surpasses that of every other entertainment industry (Statista). In this context, it appeared to us as a worthwhile avenue of study. Such things as cryptography and artificially created languages have historically been used to great effect in literature and film which makes this investigation not without spiritual precedent.

Results and discussion

1. Virtual reality

Virtual reality provides new opportunities for creating unique containers. In our preliminary research, we have already described how unique interaction between the physical and virtual spaces occupied by user creates opportunities of hiding information in physically illegal virtual spaces (inside solid virtual objects, inside the walls, below the floor). While this presents to us a notable example of using VR for what we would have to classify as virtual physical steganography (a real-life equivalent would be using a hidden cache), there are many additional prospects of using VR spaces for the purposes of linguistic steganography proper [Dzhunkovskiy, 2019].

Applications such as VRChat are based on communication. They are in essence VR-versions of social spaces feature-complete with voice chat,

motion controls, in-depth avatar customization, and the ability to create new interactive spaces, e.g., galleries, movie theaters, clubs, music venues, gaming spaces. This provides perfect basis for online socialization, which was especially notable during the pandemic. Such products based on socialization and communication create many opportunities for using linguistic steganography (VRChat).

A considerable advantage of using VR-spaces as a medium for relaying containers with stego is the inherent difficulty of setting up, maintaining and using VR. Additionally, prolonged use may be hazardous, is not recommended, and requires vast user experience and training. This facilitates a situation in which steganalysis becomes inconvenient and taxing on the analyst in addition to being difficult. We posit that using currently existing steganographic methods in VR without many additional alterations may already provide benefits to the security of the confidential information relayed, although this claim clearly requires additional research.

A notable aspect of these VR-spaces is that oral speech is prevalent over text. While written digital texts certainly exist in these spaces, most of the communication is oral using microphones and audio output devices integrated into VR-headsets. It is also possible to emote and gesticulate using hand-tracking controllers, making silent communication using gestures possible. A caveat to this is that only some devices support finger-tracking and currently none track and relay eye movement and facial expressions.

While it is plausible that audio may be covertly recorded by either the application or the VR-set itself for possible future analysis (including steganalysis), it appears dubious that the same would apply to gestures. While hand-tracking controller location data is most likely available to third parties, interpreting this data would prove an arduous task.

This brings us to the conclusion that it would be prudent to create a gesture-based system for linguistic steganography purposes in VR. In essence this would be a continuation of our concept of "trigger-containers" where one particular communication event is meant to hold additional meaning that is known to both the sender and the recipient and is agreed upon beforehand.

Traditional methods of steganography may also be used; however, we highlight the susceptibility of all conversations to being recorded in VR for future analysis without user knowledge or consent.

2. Digital governance

One of the areas of application of steganographic technologies is the field of public administration and, more precisely, digital governance. Let us turn to the analysis carried out by H. Si [Si, 2007].

The authors of the study note that one of the key features of e-government is the transfer of confidential data through computer networks. Certain data must be protected at the same level as matters of national security. Although each digital government has internal networks, none of them can forego using the Internet. Such an attempt would mean, according to the authors, a waste of resources. At the same time, the Internet is an open environment, and therefore the protection of data transmitted through the network is an important issue in the context of digital government.

This point of view is quite consistent with the state of affairs in Russia. E-government is not only becoming an important element of public life in large cities, but also of great importance in a country-wide environment, potentially creating a solution to a number of complex logistical issues. There is no doubt, however, that it is premature to talk about a complete transition to digital governance. Nevertheless, ensuring security in this area is a matter of national importance for any state wishing to develop technology in this field.

It is further noted that all governments interested in information security hire cryptographers and spend a large amount of both resources and time developing specialized information systems and advanced cryptosystems to increase the level of data security.

They further note that cryptography is not suitable for certain purposes. With the increase in computing power and the development of cryptoanalysis techniques, modern cryptosystems cannot and will not remain relevant forever. This is also consistent with our observations, but it should be noted that perhaps the authors are overly critical when deliberating on the topic of

cryptography. We believe that cryptography can become an additional element of protecting confidential information in synthesis with steganography as an additional layer of secondary protection.

The authors emphasize that voting is an important tool for assessing public opinion. Concerns about the effectiveness, accuracy and fairness of traditional paper ballot elections have always existed. Electronic voting systems have been in development for many years to overcome these concerns. However, the possible effect of security breaches in electronic voting systems is much higher than in traditional systems. The use of fingerprint technology may be an important factor in alleviating existing concerns.

We would like to point out that fears of this kind are indeed justified. This means that creation of the most durable steganographic protection systems possible is an issue that requires research.

The authors also mention the use of steganography in anonymous whistleblower systems to enable governments to fight corruption and crime. The common thread between these two examples is that people do not want to disclose their identity, and the government must ensure that anonymous activities are reliable and not malicious.

Some other studies propose the concept of anonymous fingerprints [Pfitzmann, Waidner, 1997]. A third party, namely the registration authority, informs the government of its signature, and the anonymous user registers with the authority through a registration protocol, in which they must verify their identity and receive a certificate from the authority. This certificate is registered in the center, but does not contain publicly retrievable information about the holder.

During voting or notification, the anonymous user and the state interact within the framework of a multilateral protocol: the anonymous user must provide their certificate signed by the center and receive a receipt with a digital fingerprint. The government deduces the digital fingerprint from the anonymous certificate and retains it as proof of conversion, but does not actually have any knowledge of the anonymous user's identity. However, if further verification is needed, the government can extract the certificate identification data from the digital fingerprint and provide it to the registration center as proof of the relevant identity. This issue was also considered in other studies [Pfitzmann, Sadeghi, 2000].

The flipside of the development of steganographic technologies is the issue of state regulation. The current status quo shows that the state is seeking to legally limit the power of cryptographic systems available to the general public and the market. This policy is explained by the need to prevent terrorist and criminal organization activities. In case of proper development of steganographic technologies, it will be important to develop steganalytical technologies to prevent cases of their use for illegal purposes.

3. Recreation

To consider the uses of steganography in recreation is to be cognizant of two important trends: gamification and recreational use of non-recreational cultural artifacts.

Gamification is one of the modern trends in education technologies. It appears that introducing game elements to the process of acquiring a skill makes the process more enjoyable and easier for the learner.

The second trend can be thus elucidated using the following example: in cultural history, cryptography has been widely used for recreational purposes, e.g. "The Adventure of the Dancing Men", Sir A.C. Doyle's Sherlock Holmes story using a simple substitution cypher as an important plot device. This follows a trend of linguistic achievement used by cultural creators to enhance their works. Another notable example is creators using artificial languages for the purposes of worldbuilding (e.g., J.R.R. Tolkien's Sindarin, M. Okrand's Klingon, P. Frommer's Na'vi, D. Peterson's High Valyrian).

It appears that modern game developers have been using the medium of video games to teach basic steganography skills to users through gameplay. We were able to discover research that creates a solid theoretical (and practical) framework for this in the field of cryptography: Cryptography Professional Rival, a game that employs AI and gamification to teach users basic cryptoanalysis methods [Ivanov, Dorostkar, 2021].

Learning in this game starts with teaching the user certain math principles and algorithms and continues with solving cryptographic problems.

The game has three difficulty levels: basic, intermediate and advanced. At the basic level, the players evaluate the basics of cryptography and mathematics, at the intermediate level, they employ algorithms and problem-solving skills, and at the advanced level, they create the tasks themselves, which are evaluated by artificial intelligence.

While we were unable to acquire data in regards to how effective this method is, we have been able to find two clear examples of video game developers making steganography a main gameplay and storytelling element in their products: FEZ and Tunic.

FEZ. In 2013 the game FEZ was created by the Polytron Corporation (FEZ). In it, textual information is presented as stone monoliths with quasi-meaningless columns of symbols not dissimilar to Tetris figures. Initially, the player has no knowledge that these monoliths contain stego decryption instructions. At the time, these elements are perceived as elements of visual ambiance.

There are two information protection systems in FEZ. One of them allows the user to decipher numerals (Fig. 1).

The other system deals with letters (Fig. 2).

The way in which the user is expected to uncover the protection systems in place is rather creative (Fig. 3).

One of the in-game locations contains a monolith describing every letter of the FEZ alphabet. Next to it, there is a fox jumping over a dog. Most English speakers are meant to recognize this as the pangram “The quick brown

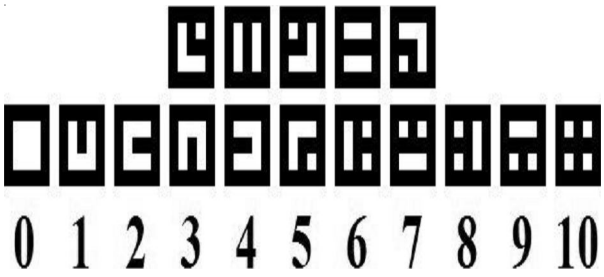

Fig. 1. FEZ numerical system

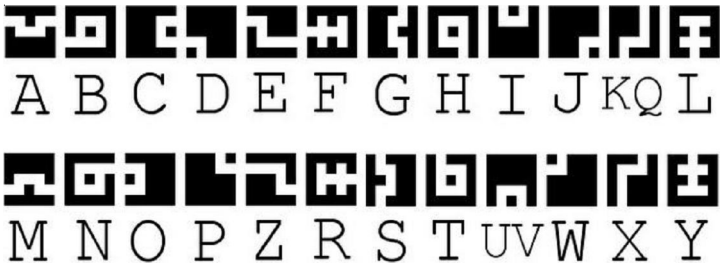

Fig. 2. FEZ alphabet system

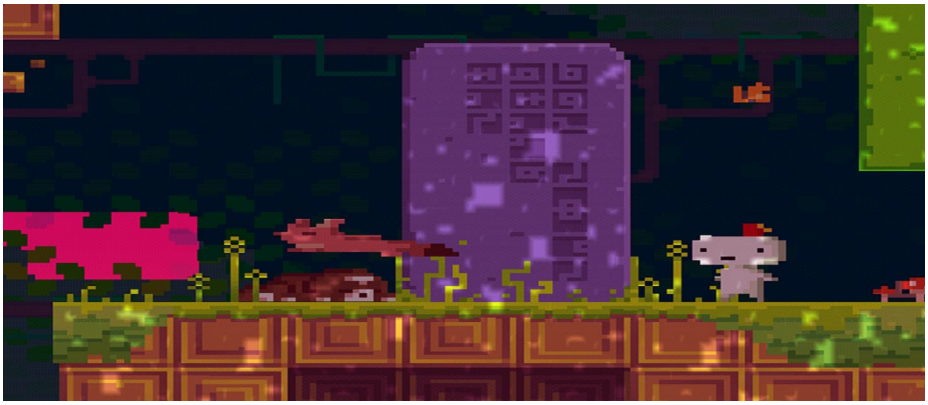

Fig. 3. FEZ “Rosetta Stone”

fox jumps over the lazy dog". By rotating the monolith 90° left, the symbols align with the phrase "The quick brown fox", granting the user enough data to decipher the rest of the alphabet.

Tunic. A fascinating case of recreational use of steganography can be found in the 2022 game Tunic created by the developer Finji (Tunic). The language used, sometimes referred to as "Trunic", is a phonetic runic steganographic alphabet.

When analyzing the Trunic language, it is first necessary to consider the alphabet. Trunic is an English-based linguistic artifact. Trunic differs from most other alphabets in two respects. First, it is phonetic. This means that it does not correspond to English letters, but to English sounds. There are 44 phonemes in English, of which 42 are included in the Trunic system. The vowel phonemes [ʌ] and [ɔ:] are not represented. Second, it is runic. Vowels merge with consonants, forming a new symbol for each combination of vowel-consonant and consonant-vowel.

The symbols in Trunic display the hexagon motif that is present throughout the Tunic world. Symbols are formed using 5 of the 6 edges of the hexagon, 6 radial lines from the center of the hexagon to each of its vertices, and a dot/circle mark at the bottom of the symbol. The symbols are oriented so that the vertex of the hexagon is at the top and bottom, and the straight edge of the hexagon is on the left. The edge that should have been on the right side is omitted so that there is no ambiguity between adjacent characters in the word.

The Trunic font is a phonetic font. Edge lines are used to represent vowels, with different combinations representing different vowels. Not all combinations are allowed – there are a total of 18 different vowels in the script. Likewise, radial lines are used to represent consonant sounds. There are 24 different consonants in the alphabet. Where a font represents pairs of voiced and unvoiced consonants (e.g., "g" and "k", "d" and "t"), the representation of one is the vertically inverted representation of the other.

It should also be noted that the phonemes of the Trunic cipher are given in IPA format. This alphabet is designed to display phonemes, intonation, syllables and word separation.

Since the representations of consonants and vowels do not overlap, characters can represent a consonant, a vowel, or both. When a character includes both, it is common for the consonant to precede the vowel. However, a small circle can be added at the bottom of the symbol to indicate that the vowel must be perceived.

Individual characters may be displayed in a regular hexagon shape, but in most cases, they are displayed in a hexagonal shape that is about twice as high as it is wide. Regardless of the shape used, the Trunic font is monospaced – all characters are the same width.

When printed, they usually split into top and bottom at a point slightly below the middle of the character. These parts appear above and below a character as a solid horizontal line that spans the width of the character. The top part touches the line, while the bottom part is slightly below the line, creating a visible break in the character. When hand-written, the horizontal line and break are sometimes omitted.

Numbers written in Trunic font can be voiced (similar to writing "two" instead of "2") or represented by Arabic numerals.

Words are made up of a series of symbols representing the sounds that the word makes when spoken aloud, in order from left to right. Each character slightly overlaps the character before it, so that the left edge of the second character matches where the right edge of the first character should be. As a result, lines from one character often flow smoothly into the lines of the next character. When a horizontal line is displayed, it appears as a solid line through all the characters in the word.

Sentences are written as strings of words with spaces (about half the width of a character) between them. Sentences end with dots, which can be represented as small circles instead of simple dots. Some other punctuation marks are carried over from normal English writing (for example, commas), but punctuation marks that occur in a word (for example, apostrophes denoting possessive or contractive) are always omitted.

Words written in the English alphabet mix freely with words written in the Trunic script, although the two representations never mix within the same word.

When forming a consonant sound, internal ribs are used. No consonant symbol uses a central edge unless the top and bottom edges have an edge to join (see Fig. 4).

Within gameplay, the user has access to an incomplete manual that is written in English and Trunic. Throughout the game, the user acquires more pages of the manual that allows them to solve more secrets. Completing the game is impossible without fully interpreting the Trunic alphabet. At one point, the user will be guided to the epiphany that one of the pages contains a Rosetta stone artifact depicting a graphic equivalency between some items and their names in Trunic (Fig. 5).

This process of language decryption mirrors that previously observed in FEZ and might provide a robust framework for crypto- and steganalysis skill instruction.

Conclusion

We managed to identify a number of linguistic steganography uses outside of traditional covert confidential information relay in VR, digital governance and recreation.

The optimal way to implement linguistic steganography into VR is the use of gestures inside the virtual world. This is made possible by hand tracking technology in the controllers and synergizes well with trigger-container method of linguistic steganography where the stego is agreed upon by the parties beforehand and the gesture acts as the impulse to "perceive" the message in question. On

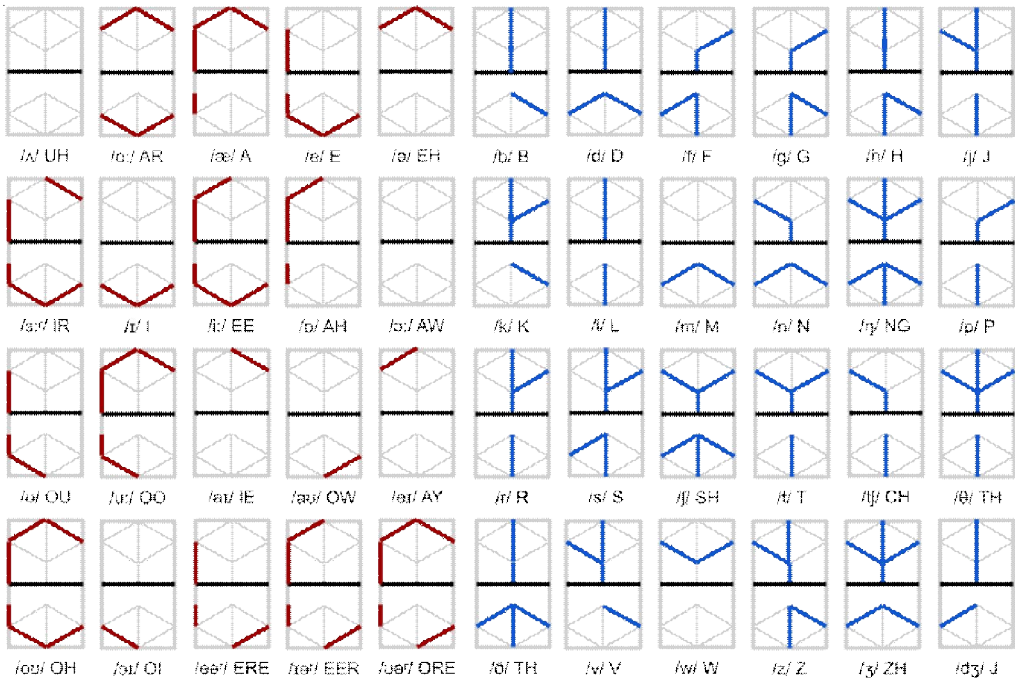

Fig. 4. Trunic phonetic runic alphabet

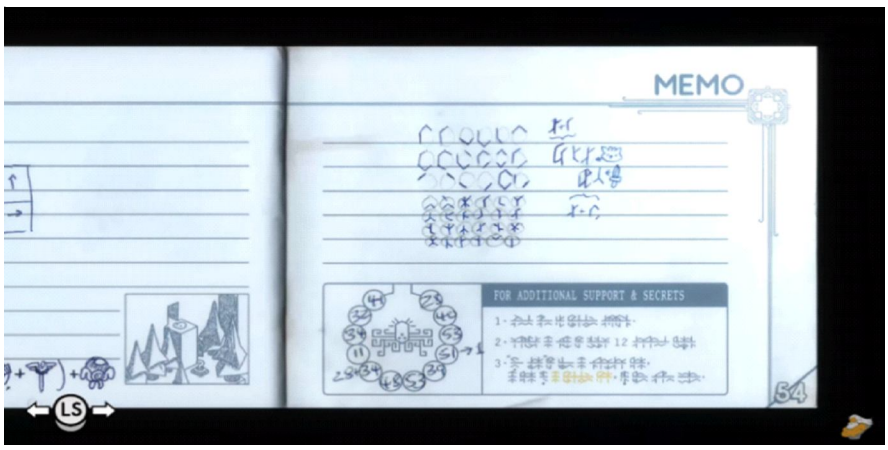

Fig. 5. Trunic Rosetta stone

top of that, VR environments create unique opportunities for digital physical steganography.

It appears that steganography may be crucial to digital governance when considering electronic voting and combating corruption. This is especially noteworthy in the pandemic/post-pandemic contexts where many traditional services become optimal in their remote and digitized forms.

Finally, it appears that there is large potential in using computer games as a tool for teaching users basic steganography and cryptography skills. This aligns well with the current trend of gamification in education and edutainment.

Additional continuous monitoring and analysis is required to determine more avenues of using steganographic technologies for non-traditional purposes. Within the context of applied linguistics and interdisciplinarity, we may discover new productive ways of adapting these technologies for various goals.

REFERENCES

Alferov A.P., Zubov A.Yu., Kuzmin, A.S., 2012. *Osnovy kriptografii* [Basis of Cryptography]. Moscow, Gelios ARV Publ. 480 p.

Dzhunkovskiy A.V., 2018. Steganography: Three-Stage Analysis Methodology Applied to Russian Written Texts. *Vestnik MGLU. Gumanitarnye nauki* [Vestnik of Moscow State Linguistic University. Humanities], no. 6 (797), pp. 117-123. DOI: https://doi.org/10.18454/RULB.2021.26.2.10

Dzhunkovskiy A.V., 2019. Prospects of Using VR Technologies as a Steganography Medium. *Vestnik MGLU. Gumanitarnye nauki* [Vestnik of Moscow State Linguistic University. Humanities], no. 7 (823), pp 155-166.

Ivanov S.G., Dorostkar Z., 2021. Professionalnyy sopernik kriptografii (PSK): model razrabotki igr dlya izucheniya kriptografii [Professional Rival (CPR): A Game Designing Model to Learn Cryptography]. *XXIV Mezhdunarodnaya konferentsiya po myagkim vychisleniyam i izmereniyam* [The 24th International Conference on Soft Computing and Measurments]. Saint Petersburg, State Electrotechnical University "LETI" im. V.I. Ulyanova (Lenina), pp. 312-315.

Kamaruddin N., Kamsin A., Por L.Y., Rahman H., 2018. Review of Text Watermarking: Theory, Methods, and Applications. *IEEE Access*, no. 6, pp. 8011-8028. DOI: 10.1109/ACCESS.2018.2796585

Pfitzmann B., Sadeghi A.-R., 2000. Anonymous Fingerprinting with Direct Non-Repudiation. *Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security, December, Kioto*. Berlin, Heidelberg, Springer , pp. 401-414.

Pfitzmann B., Waidner M., 1997. Anonymous Fingerprinting. Fumy W., eds. *Advances in Cryptology – EUROCRYPT '97. EUROCRYPT 1997. Lecture Notes in Computer Science. Vol. 1233*. Berlin, Heidelberg, Springer. DOI: https://doi.org/10.1007/3-540-69053-0_8

Potapova R.K., Dzhunkovskiy A.V., 2020. Preliminary Investigation of Potential Steganographic Container Localization. *Lecture Notes in Computer Science*, no. 12335, pp. 389-398. DOI: https://doi.org/10.1007/978-3-030-60276-5_38

Potapova R.K., 2002. Lingvisticheskie znaniya i novye tekhnologii [Linguistic Knowledge and New Technologies]. *Akusticheskiy zhurnal* [Acoustic Physics], vol. 48, no. 4, pp. 552-559.

Potapova R.K., 2010. *Rech: kommunikatsiya, informatsiya, kibernetika* [Speech: Communication, Information, and Cybernetics]. Moscow, URSS Publ. 600 p.

Si H., 2007. Maintaining Information Security in E-Government Through Steganology. *Encyclopedia of Digital Government*. Uorik, IGI Global, pp. 1180-1184. DOI: 10.4018/978-1-59140-789-8.ch178

Van Tilborg H., ed., 2014. *Entsiklopediya kriptografii i bezopasnosti* [Encyclopedia of Cryptography and Security]. Berlin, Springer, Science and Business Media. 1416 p.

Wayner P., 2009. *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*. San-Francisko, Morgan Kaufman Publ. 155 p.

SOURCES

FEZ – *FEZ osnovnaya stranitsa* [FEZ Homepage]. URL: https://store.steampowered.com/app/224760/FEZ/

History... – History of Virtual Reality: Timeline. *Verdict*. URL: https://www.verdict.co.uk/history-virtual-reality-timeline

Statista – Video Game Industry – Statistics and Facts. *Statista*. URL: https://www.statista.com/topics/868/video-games/#topicOverview

Tunic – *Tunic Homepage*. URL: https://store.steampowered.com/app/553420/TUNIC/

VRChat –*VRChat Homepage*. URL: https://hello.vrchat.com

Information About the Author

Andrey V. Dzhunkovskiy, Candidate of Sciences (Philology), Head of the Department of Applied and Experimental Linguistics, Senior Researcher, Experimental Phonetics Laboratory of Forensic Linguistics, Moscow State Linguistic University, Ostozhenka St, 38, Bld. 1, 119034 Moscow, Russia, Vetinari01@gmail.com, https://orcid.org/0000-0002-3761-8010

Информация об авторе

Андрей Владимирович Джунковский, кандидат филологических наук, заведующий кафедрой прикладной и экспериментальной лингвистики, старший научный сотрудник экспериментально-фонетической лаборатории криминалистики по речеведению, Московский государственный лингвистический университет, ул. Остоженка, 38, стр. 1, 119034 г. Москва, Россия, Vetinari01@gmail.com, https://orcid.org/0000-0002-3761-8010